(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－106149

(43)公開日　平成10年(1998)４月24日

(51)Int.Cl.[6]	識別記号	FI	
G11B 20/10		G11B 20/10	H
15/087		15/087	E
	301		301
H04N 5/91		H04N 5/91	P
5/92		5/92	H

審査請求　未請求　請求項の数21　ＯＬ　（全 10 頁）

(21)出願番号　特願平9－193455

(22)出願日　平成９年(1997)７月18日

(31)優先権主張番号　０８／６９０７０６

(32)優先日　1996年７月31日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

(72)発明者　チャールズ・ヘンリィ・ペネット
アメリカ合衆国10520、　ニューヨーク州　クロトンーオンーハドソン　メモリィ　レーン　５

(74)代理人　弁理士　坂口　博　（外１名）

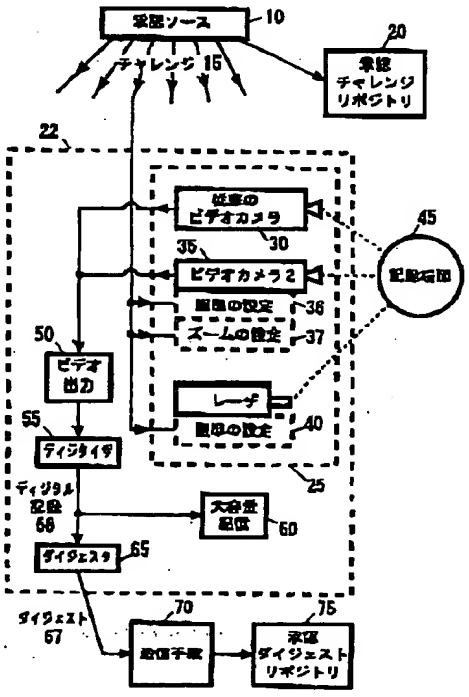
最終頁に続く

(54)【発明の名称】　認証可能なディジタル記録を作成する装置および方法

(57)【要約】　（修正有）

【課題】　先日付、後日付または変更を行うことができず、または予め記録した材料を組み合わせることによって容易に電子的に作成することのできないビデオテープ、音声記録、ログ等の記録を作成する装置の提供。

【解決手段】　不正な変造を防止するためカメラまたはその他の記録装置が承認ソース１０から予測不可能であることが保証されている信号（「チャレンジ」）１５を周期的に受信しこれらの信号によって記録中の場面に影響を及ぼし、次に進行中のディジタル記録のダイジェストを承認リポジトリ７５に周期的に転送する。この予測不可能なチャレンジによって、このチャレンジの受信以前の時刻に記録を先日付にすることが防止され、一方ダイジェストの格納によって、このダイジェストをリポジトリが受信した時刻以降に上記記録を後日付にすることが防止される。



1

【特許請求の範囲】

【請求項1】認証可能なディジタル記録を作成する記録装置であって、

周期的に送信され且つ第1の承認リポジトリに格納される予測不可能な信号に応答し、記録可能な効果を生じるように記録中の証拠に影響を及ぼす受信手段と、

上記記録可能な効果を含む上記証拠を記録し、ディジタル記録信号を発生する記録手段と、

上記ディジタル記録信号から取り出した認証情報を第2の承認リポジトリに送信して格納する送信手段とを含み、

上記第1の承認リポジトリに上記予測不可能な信号を格納した時と上記認証情報を上記第2の承認リポジトリに格納した時とによって定まる期間は、リアルタイムで上記効果をシミュレーションするのを困難または不可能にするのに十分短いことを特徴とする記録装置。

【請求項2】上記ディジタル記録信号を格納する大容量記憶装置と、

上記ディジタル記録信号を受け取り上記ディジタル記録信号の1つ以上のディジタル・ダイジェストを発生するダイジェスタと、

を更に有することを特徴とする請求項1記載の記録装置。

【請求項3】上記ディジタル記録信号を格納する大容量記憶手段を更に有することを特徴とする請求項1記載の記録装置。

【請求項4】上記記録手段は証拠を記録するビデオ・カメラを含むことを特徴とする請求項1記載の記録装置。

【請求項5】上記記録手段は上記受信手段の受信した信号によって制御される照準及びズームの設定を有する補助カメラを更に有することを特徴とする請求項4記載の記録装置。

【請求項6】上記記録手段は照準および強度が上記受信手段の受信した信号によって制御される良好な平行度を有するビームを放射するレーザを更に有し、上記レーザは記録した証拠に効果を生じることを特徴とする請求項4または5記載の記録装置。

【請求項7】上記記録手段は、

上記受信手段の受信した信号によって制御されるプロンプト発生器と、

上記プロンプト発生器によって制御され、協力者に動作を促すためのプロンプトを上記協力者に出す手段と、

を更に有することを特徴とする請求項4記載の記録装置。

【請求項8】上記プロンプトは、ビデオ・プロンプトまたは音声プロンプトであることを特徴とする請求項7記載の記録装置。

【請求項9】上記記録手段は、

上記受信手段の受信した信号によって制御されるプロンプト発生器と、

2

上記プロンプト発生器によって制御され、協力者による自発的な反応を生じる知覚信号を上記協力者に対して発生する手段と、

を更に有することを特徴とする請求項4記載の記録装置。

【請求項10】上記知覚信号は可視信号または可聴信号であることを特徴とする請求項9記載の記録装置。

【請求項11】上記予測不可能な信号を周期的に送信する承認ソースを更に有することを特徴とする請求項1記載の記録装置。

【請求項12】上記信号は、物理的ランダム・プロセス、疑似ランダム・プロセス、または完全には予測することのできない公に検証可能なデータから発生されることを特徴とする請求項11記載の記録装置。

【請求項13】上記第1の承認リポジトリは上記承認ソースと組み合わされることを特徴とする請求項11記載の記録装置。

【請求項14】予測不可能な信号の承認ソースと、

上記信号を保存し、上記信号を受信した時を保証する第1の承認リポジトリと、

上記信号に応答し、記録中の証拠に上記信号の効果を及ぼすようにディジタル記録を作成するディジタル記録装置と、

上記ディジタル記録から取り出した認証情報を保存し、上記認証情報を受け取った時を保証する第2の承認リポジトリと、

を有することを特徴とする認証システム。

【請求項15】上記ディジタル記録を受信して上記認証情報である1つ以上のダイジェストを発生するダイジェスタを更に有することを特徴とする請求項14記載の認証システム。

【請求項16】上記ディジタル記録を格納する大容量記憶装置を更に有することを特徴とする請求項15記載の認証システム。

【請求項17】上記信号の少なくとも1つを発生した時と、上記信号によって影響を受けたディジタル記録を上記第2の承認リポジトリによって受信した時との間の時間間隔は、上記効果の組立またはシミュレーションを不可能にするほど短いことを特徴とする請求項14記載の認証システム。

【請求項18】上記ディジタル記録装置はビデオ・カメラまたは音声記録器を有することを特徴とする請求項14記載の認証システム。

【請求項19】第1の承認リポジトリに格納される送信された予測不可能な信号を受信し、該信号の効果を記録中の証拠に及ぼすステップと、

上記効果を含む上記証拠を記録し、ディジタル記録を発生するステップと、

上記ディジタル記録から取り出した認証情報を第2の承認リポジトリに送信して格納するステップとを含み、

上記第１の承認リポジトリに上記信号を格納した時と上記認証情報を上記第２の承認リポジトリに格納した時とによって定まる期間は、リアルタイムで上記効果をシミュレーションするのを困難または不可能にするのに十分短いことを特徴とするディジタル記録方法。

【請求項２０】上記ディジタル記録のディジタル・ダイジェストを上記認証情報として発生するステップを更に有することを特徴とする請求項１９記載のディジタル記録方法。

【請求項２１】承認ソースから上記信号を周期的に送信するステップと、

上記信号およびその送信時刻を受信して上記第１の承認リポジトリに格納するステップと、

を更に有することを特徴とする請求項１９記載のディジタル記録方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は一般的に記録した証拠の認証に関し、更に詳しくは、承認ソースから記録中の証拠に影響を及ぼす予測できない信号（チャレンジ）を周期的に受信し、承認リポジトリに対して進行中のディジタル化して記録した証拠のハッシュ・ダイジェストを速やかに転送する記録装置および方法に関する。

【０００２】

【従来の技術】犯罪の場面、警察官による面接、及び契約、規則、法令または条約を作成する場合に行われる行為のビデオテープのような記録された証拠は、この記録時に立ち会った立会人の証明によって一般的に認証され、この記録が行われた時からそれが証拠として使用される時までの間、破壊されることのないチェーンを付けて保管される。もしこの保管用のチェーンが破壊された場合、例えば、この記録が節操のない人物によって数日間貸し出された場合、最近のディジタル信号処理技術では、内部のタイム・スタンプを変更することによってまたは場面、被写体、音、データ等を付加するかまたは取り除くことによってこの証拠を作り替えることが可能である。

【０００３】従来技術は、タイム・スタンピングとして知られる技術によって種々この問題に取り組んできた。例えば、米国再発行特許第ＲＥ３４９５４号は、ハッシュ・ダイジェストを形成するための一方向ハッシュ関数を使用してディジタル文書をハッシュするタイム・スタンピング技術を開示している。このダイジェスト（２進数）を承認証明機関に転送し、この機関はこのダイジェストにタイム・スタンプを割り当て、このダイジェストとタイム・スタンプの組み合わせを暗号化するために公開鍵による暗号システムを使用する。後程この機関の公開鍵を使用してこの組み合わせを暗号解読することによって、この機関が事実ハッシュ・ダイジェストとタイム・スタンプを組み合わせたことを立証することができる。この機関には信頼性があるから、ハッシュ・ダイジェストはタイム・スタンプに対応する時点でこの機関に引き渡されたことを推論することができる。一方向ハッシュ関数の性質上、他の文書が同一のハッシュ・ダイジェスト値を有することはないと言える。

【０００４】上記米国再発行特許の方法は、所与のディジタル文書が特定の日時に機関に引き渡されたことを認証する。これは、この文書とこの文書が忠実に表そうとしている物理的世界の１組の環境との間の関係に付いて何も述べていない。例えば、ある場面を日時Ａに設定してビデオテープに記録してこれをそれより後のタイム・スタンプＢによって認証しても、これはＢ以前のある所望の日時に発生した出来事を表すものであると偽って主張することができる。または、異なった日時（全てＢよりも前）に制作した複数の部分からビデオテープを組立てることができる。従って、上記米国再発行特許の方法はビデオを制作した日時を確定する方法を提供するものではなく、単に制作した最新の日時（即ち、Ｂ）を認証するだけである。

【０００５】ある出来事がその意図する日時以前には発生しなかったことを知ることの重要性は、保険詐欺の形で示すことができる。たとえば、自分の過失に起因しない事故に巻き込まれたドライバが自分の破損した車の写真を撮り、その破損の大部分は自分の過失によって以前に発生し、保険会社に報告していない事故によって発生したものであることを秘匿してこの写真を自分の保険会社に提出した場合である。

【０００６】記録を認証するための他のアプローチは、米国特許第４９２２３３９号に開示されている。ここに開示されているのは、目視による監視と文書化を行うシステムであり、このシステムは事象を可視的に記録する１台以上のカメラとこの事象に関する（不可視）情報を取り出す変換器によって構成される。可視信号と情報信号を統合して第３の信号を形成し、この信号を記録または表示する。これは可視部分と情報部分の何れも他の部分から独立して変更することができないような方法で行われる。一例としてあげることのできるのは、ある物を計量して、その計量結果とその物の可視画像とを組み合わせるものである。タイムスタンピングはオプションである。

【０００７】上記米国特許は、ビデオ画像を物理的世界に関してある測定された情報と可能ならタイム・スタンプを含んでリンクする変更不可能な記録を提供することを主張しているが、変更不可能性を保証する何等の手段も提供していない。上記米国特許は市販の装置を使用して２つの信号を結合して１つの信号を形成することにその基礎をおいているが、この結合した信号を分解し、構成要素の１つを変更して再構築することによって新しく結合した信号を作ることができる可能性を考慮していない。例えタイム・スタンプを使用したとしても、上記米

国特許ではこのタイム・スタンプの認証を行っていない。タイム・スタンプの認証は勿論周知であるが、例えこれを上記米国特許のシステムに適用しても、かかる認証は記録を行うことのできた最新の日時を提供するに過ぎないものである。

【０００８】

【発明が解決しようとする課題】従って、本発明の目的は、日付を実際よりも前または後にしたり、内容も変更したりすることができず、また予め記録した材料を組み合わせることによって容易に電子的に組み立てることのできないビデオテープ、音声記録、ログ等の記録を作成する装置を提供することである。

【０００９】

【課題を解決するための手段】本発明によれば、上述のような記録の変造を防止するためカメラまたはその他の記録装置が承認ソースから予測不可能であることが保証されている信号（「チャレンジ」）を周期的に受信し、これらの信号によって記録中の証拠に影響を及ぼし、次に進行中のディジタル記録のダイジェストを承認リポジトリに周期的に転送する。なお「承認（トラステッドともいう）」とは、コンピュータ・セキュリティの分野で、十分な保護が図られていることを意味する。この予測不可能なチャレンジによって、記録した証拠の日付をこのチャレンジの受信以前の時刻にすることが防止され、一方ダイジェストの格納によって、記録した証拠の日付をこのダイジェストをリポジトリが受信した時刻以降にすることが防止される。一方、チャレンジと記録中の証拠との相互作用によって、記録した証拠のリアルタイムによる変造に対して強力な障害が提供され、これによって変造しようとする者はチャレンジの到達した時刻とダイジェストをリポジトリに格納した時刻の間の短い時間間隔内でこの相互作用の効果をシミュレーションせざるをえない。

【００１０】

【発明の実施の形態】図を参照して、特に図１は本発明の好適な実施例による記録装置のブロック図を示す。承認ソース１０は１つ以上の受信機に対して予測不可能なディジタル信号即ち「チャレンジ」を周期的に発生するが、図示例では上記受信機を２台示している。好適な実施例では、これらのチャレンジは物理的ランダム・プロセスによって発生するが、その一例は破壊近くまで逆バイアスされたダイオードから発生する電気的ノイズである。標準的なディジタル・サンプリング技術では、このようなプロセスを使用して各ビットが原則として殆ど完全に予測不可能なビット・シーケンスを発生することができる。このようなビット・シーケンスは、例え発生装置の設計、その初期ディジタル状態およびその過去の出力に関する完全な知識を与えられたとしても、予測することはできない。承認ソース１０は、ラジオ送信機、モデム付き電話またはコンピュータ・ネットワークのような送信手段を有することができる。

【００１１】受信機の中には、過去に送信された信号とその送信時刻を格納する承認チャレンジ・リポジトリ２０、および１つ以上の認証用ビデオ・カメラ・アセンブリ２５が含まれる。以下でより詳細に説明するように、承認チャレンジ・リポジトリ２０は承認ソース１０または承認ダイジェスト・リポジトリ７５と結合することができ、またこれら３つの機能全てを１つの場所にまとめることもできる。例えば、承認チャレンジ・リポジトリ２０は「受信機」である必要はなく、これは承認ソース１０と統合してもよい。

【００１２】点線２２で囲まれた要素を有する対話型ディジタル記録装置（ＩＤＲＡ）は承認ソース１０からチャレンジ１５を受信し、記録した場面４５のディジタル記録６６と１つまたは複数のダイジェスト６７を発生し、これらのダイジェストを承認ダイジェスト・リポジトリ７５に転送する。好適な実施例では、ＩＤＲＡは、ビデオ・カメラ・アセンブリ２５、ビデオ出力５０、ディジタイザ５５、大容量記憶媒体６０およびダイジェスタ６５によって構成する。

【００１３】認証用ビデオ・カメラ・アセンブリ２５は、通常の照準、ズーム及び焦点を有する従来のビデオ・カメラ３０と、照準３６およびズーム３７の設定がメイン・カメラ３０のそれらに対してチャレンジによって制御される補助カメラ３５と、照準および強度をチャレンジによって制御され良好な平行度を有するビームを放射する赤外線レーザ４０とで構成する。例えば、１秒に１回受信される６４ビットのチャレンジは２つの３２ビット・ワードに分割することができる。第１のワードは、レーザ４０に対して2^{32}の可能な走査パターン（これらの走査パターンの各々は最後のチャレンジ以降１秒の間隔の間に場面の大部分を数回巡回しなければならない）からの選択を指定するために使用することができる。第２のワードはメイン・カメラ３０に対する補助カメラ３５の2^{32}の可能な照準およびズームからの選択を与えるものである。

【００１４】変造しようとする者が、予め記録した場面上にレーザ光が発生し得る効果をコンピュータ・グラフィックスによって得ようとする場合、レーザ４０の予測不可能な走査パターンはこの者が大量の演算資源を消費することを要求する。予測不可能なズームは、変造しようとする者に対し、記録した場面の各部分の詳細に関する現実の証明可能な情報の大量のデータベースを保持することを要求する。

【００１５】アセンブリ２５は、認証すべき場面４５のビデオ記録を捕捉し、それに対して上述の変更および操作が加えられる。アセンブリ２５から出たビデオ信号５０は従来設計のディジタイザ５５によってディジタル化され、その後このディジタル化した信号は、あとで検索するために、磁気テープ、ディスク等の大容量記憶媒体

６０に格納される。ディジタイザ５５の出力はダイジェスタ６５にも供給される。ダイジェスタ６５は安全なハッシュ関数を使用して現在または累積のディジタル信号６６のダイジェストを周期的に準備する。ハッシュ関数の正確な形式は、新聞またはコンピュータ・ネットワークの複数のサイトに対して行う配布による公表によって予め告知するかまたは公の合意を取り付ける。もし５１２ビットを２５６ビットに写像する安全なハッシュ関数ｈを使用すれば、ディジタル化したビデオ信号を２５６ビットのブロックB_1，B_2，・・・B_nに分割し、以下の反復によってダイジェストD_nを演算することによって１秒間の動作のダイジェストを計算することができる。

$D_0=0$

$D_1=h\ (B_1,\ D_0)$

$D_2=h\ (B_2,\ D_1)$

・

・

・

$D_n=h\ (B_n,\ D_n-1)$

各秒の終了時点に於いて、チャレンジの効果を含む過去の全ビデオ記録に依存する現在のダイジェストＤｎは伝送手段７０によって承認ダイジェスト・リポジトリ７５に伝送され、その受信時刻および他の識別情報と共に格納される。

【００１６】上記のプロセスは、図２の流れ図に要約してある。機能ブロック１００に示すように、予測不可能なディジタル信号（即ち、チャレンジ）を承認ソース１０によって周期的に同報通信する。これらの信号は、機能ブロック１０５に於いて承認チャレンジ・リポジトリ２０に受信され、格納される。これらの信号はまたビデオ・カメラ・アセンブリ２５にも受信される。ビデオ・カメラ・アセンブリ２５はこれらの信号を使用して機能ブロック１１０でカメラ３５を制御すると共に機能ブロック１１５でレーザ４０を制御する。その結果、機能ブロック１２０で変更された場面が記録され、機能ブロック１２５でディジタル化する。ディジタル化した信号は機能ブロック１３０で大容量記憶媒体６０に格納し、これはまた機能ブロック１３５に於いてハッシュ関数を使用してダイジェスタ６５によってダイジェストする。このダイジェストは、次に機能ブロック１４０で承認ダイジェスト・リポジトリ７５に送信する。

【００１７】従って、本発明による対話型記録装置は、記録を行った時刻からその認証時刻までの期間を定める。この期間を短くする（例えば１秒）ことによって、変造しようとする者がリアルタイムでチャレンジの記録された効果をシミュレートするのが困難または不可能になる。

【００１８】幾つかのケースでは、記録すべき証拠および上述の期間は、協力者（完全に協力的でなくても構わない）と共に小さく取り囲まれた空間（例えば、スタジオ）で記録した１人または複数の人物の場面である。このようなケースの場合ビデオ・カメラ・アセンブリ２５には、図３に示すように、別の装置を付加してもよい。この装置は、記録した証拠を認証するためこの場面に影響を及ぼしまたはこの場面を変更するために使用することができる。例えば、ビデオ・モニタ３１０は、ある言葉を発するかまたは特定の動作（例えば、右手を挙げる）等の予測することのできない命令を協力者に対して表示することができる。これらの動作はチャレンジ信号１５に応答してプロンプト発生器３１１がデータベースから選択するが、これは周知のパソコン技術の簡単な応用である。スピーカ３２０は、モニタ３１０と同じプロンプトを発生することができる。または、これは、記録した証拠で検出可能なように、不意に協力者を驚かす大きな音響を短時間発生することができる。スピーカ３２０は、同じプロンプト発生器３１１によって駆動することができる。

【００１９】また、投光器３３０を設けることができ、これを使用して場面の照明に緩慢な変化を持たせ、または短時間明るい光を発して協力者に記録可能な刺激による反射運動を起こさせてもよい。これらの投光器は、プロンプト発生器３１１および可変電源３３１の両方によって制御することができる。電源３３１も予測不可能なチャレンジ１５によって制御する。通常の扇風機３４０は、その速度が変化することによって協力者の衣服や髪の毛またはこの場面にあるその他の可動部分を記録可能な方法で乱すことができる。投光器３３０と同様に、扇風機３４０もプロンプト発生器３１１および可変電源３３１の両方によって制御することができる。

【００２０】図１に示すビデオ・カメラ３５およびレーザ４０の場合と同じく、プロンプト発生器３１１および可変電源３３１については、入力した予測不可能なチャレンジとこのチャレンジによって発生する物理的動作の間のマッピングは、新聞またはコンピュータ・ネットワークの複数のサイトに対して行う配布による公表によって予め告知するかまたは公の合意を取り付ける。信号がランダムに入力される結果ランダムなチャレンジが発生することを普通の人なら誰でも気づくことができるように、このマッピングは十分簡単でなければならない。例えば、「もし１が連続して５個入力されれば、扇風機の速度が増加し、もしゼロが連続して５個入力されれば扇風機の速度を落とす」といった規則を使用することができる。

【００２１】ビデオによる記録を説明してきたが、本発明は音声による記録にも適用可能である。音声記録も、もし適切に認証することができなければ、その内容を操作することが可能である。レーザによる走査の代わりに、チャレンジによって大きなクリック音またはその他の音がラウドスピーカのフェーズドアレイから発生し、

記録が行われている部屋またはその他の環境からチャレンジに応じた反響音を発生する。補助カメラのズーミングおよび照準合わせの代わりに、チャレンジは記録を行っている１個または複数個のマイクの移動を指定することができる。もし記録に協力者が含まれていれば、ビデオの場合と同様に、チャレンジは指定した単語または句、あるいはその他の指定した音を発するよう協力者に指示することができる。

【００２２】帯域幅が狭いため、一般的に音声による記録はビデオによる記録と比較してより速やかに操作して変造することができる。従って、１個だけでなく数個のマイクを使用すること、及び主観的に忠実な音声記録に必要である以上の振幅および時間解像度によって音声信号を変換及びディジタル化することによって、音声記録の帯域幅を増加するのが好ましい。その結果得られる記録には、記録中の音源とチャレンジによって誘起された特別の音に対する部屋またはその他の環境の時空間応答に関する不可聴であるが再生可能な情報が含まれている。

【００２３】更にリアルタイムで行われる変造を防止するため、チャレンジの送信とその後最初に発生するダイジェストの保管との間の時間窓をビデオの実施例で必要とするよりも短くしなければならない。例えば、これは数秒ではなく数ミリ秒にしなければならない。これは、幾つかの応答、例えば、協力者の話した応答がより長時間の規模で行われたとしても、実行可能である。この場合、１個のチャレンジに対する応答は、次の数秒分の格納したダイジェストに影響を及ぼすものである。

【００２４】本発明の他の用途は、例えば、化学工場で発生したエンジニアリング・データまたはプロセス・データのリアルタイムのログの認証である。認証されないビデオ記録と同様に、プロセス・ログを操作して、発生したとされている一連の事象を変造したり、先日付にしたり後日付にしたりすることができ、これらのログは一般に重大な事故の直後に没収される。期間を定めることによるプロセス・ログの認証は、プロセスの安全性と製品の品質を大幅に低下させないような十分小さい範囲内で、オンラインのチャレンジに応答してプロセスの制御パラメータをランダムに変調する装置によって得ることができる。プロセスを制御するために通常は使用しない他のパラメータも、より複雑でシミュレーションを行うことが困難な応答を発生するために変調することができる。同じ理由で、実際のプロセスに対する入出力関係のリアルタイムのシミュレーションを困難にするために、通常のプロセス・ログは、プロセスの制御目的のために通常監視されている出力変数以外に他の情報を十分収集することによって増大される。

【００２５】元の形ではリアルタイムでシミュレーションおよび変造を行うことのできる解像度の低い記録（例えば、帯域幅の狭いモノラルの音声記録または解像度の低いプロセス制御ログ）であっても、同じ現実の世界の事象のより解像度の高い光景にこれを埋め込むことによって、保護することができるという原理を、音声及びプロセス制御の実施例は例示し、この場合この光景は帯域幅がより広く、入出力のパラメータがより多く、これらのパラメータはより複雑な力学によって関連づけられる。

【００２６】好適な実施例にはチャレンジを発生するために原理的に予測することのできない物理的なプロセスが含まれているが、予測不可能な構成要素を有する他のプロセスをその代わりに使用してもよい。株式及び商品取引で発生する公に検証することのできる統計（例えば、所定時間内に偶数の商いが行われているか奇数の商いが行われているか）は、個人の制御能力を完全に超えているので、これらの統計を使用してランダムなチャレンジを与えることができる。秘密のシードを有する暗号的に強力な疑似乱数発生器のような決定論的プロセスでさえも、これを使用してチャレンジを発生することができる。実用上ユーザの属する階層の人々によって予測不可能なプロセスがあれば、そのようなプロセスを使用することができるが、疑似乱数発生器の場合には、シードはインサイダ情報を構成するのでそのソースの秘密が保持されているという信頼性を与える必要がある。

【００２７】上述した実施例の何れの場合にも、種々の理由のため、記録装置が離れた場所にある承認チャレンジのソースおよび離れた場所にある承認ダイジェスト・リポジトリに対する連続的なオンラインの双方向通信を維持することは実際的ではない。これらの機能の何れか一方または両方は、承認ソースまたはリポジトリの仕事を実行しようと意図する記録装置内のモジュールによってローカルで実行することができる。このような実行は、オンライン接続が必ずしも可能ではない状況で使用することができる。ローカルで実行される承認機能（ソースまたはリポジトリ）は何れも不正な介入から保護しなければならないが、これは従来設計の不正介入防止モジュール（ＴＲＭ）、例えば、侵入を導線の電気抵抗の変化によって検出する導線埋め込みエポキシ・パッケージに封入することによって行われる。オフライン動作中の先日付や後日付の防止を支援するため、例えばＴＲＭは外部から容易にリセットすることのできない安全なクロックを有する。何れの場合に於いても、信頼性のあるリポジトリに対する通信を再び行うことができるようになった場合、オフライン動作中に発生したチャレンジおよびダイジェストをそのリポジトリにバックアップするのが好ましい。

【００２８】もしディジタル記録６６の帯域幅が送信手段７０の容量を超えていないなら、大容量記憶媒体６０、ダイジェスタ６５およびダイジェスト６７を必要としない更に他の代替実施例が可能である。この代替実施例の場合には、ディジタル記録６６はダイジェストされ

ないで送信手段７０を介して承認リポジトリ７５に送られ、そこに保存される。好適な実施例と同様に、この実施例ではディジタル記録６６に応じて幾つかの情報を承認リポジトリに保存するが、この情報は記録中の事象４５を認証する機能を果たすものである。この実施例では、保存した情報はディジタル記録６６自身であり、一方好適な実施例では、これはディジタル記録６６の１つまたは複数のダイジェスト６７である。このようなダイジェストは自身で事象４５を認証するものではないが、その代わり、その事象のディジタル記録６６と組み合わされてこの認証を行い、これによってディジタル記録が記録装置と関連づけられた大容量記憶媒体６０のような信頼性のない場所に安全に格納されるのを可能にする。

【００２９】まとめとして、本発明の構成に関して以下の事項を開示する。

（１）認証可能なディジタル記録を作成する記録装置であって、周期的に送信され且つ第１の承認リポジトリに格納される予測不可能な信号に応答し、記録可能な効果を生じるように記録中の証拠に影響を及ぼす受信手段と、上記記録可能な効果を含む上記証拠を記録し、ディジタル記録信号を発生する記録手段と、上記ディジタル記録信号から取り出した認証情報を第２の承認リポジトリに送信して格納する送信手段とを含み、上記第１の承認リポジトリに上記予測不可能な信号を格納した時と上記認証情報を上記第２の承認リポジトリに格納した時とによって定まる期間は、リアルタイムで上記効果をシミュレーションするのを困難または不可能にするのに十分短いことを特徴とする記録装置。

（２）上記ディジタル記録信号を格納する大容量記憶装置と、上記ディジタル記録信号を受け取り上記ディジタル記録信号の１つ以上のディジタル・ダイジェストを発生するダイジェスタと、を更に有することを特徴とする上記（１）記載の記録装置。

（３）上記ディジタル記録信号を格納する大容量記憶手段を更に有することを特徴とする上記（１）記載の記録装置。

（４）上記記録手段は証拠を記録するビデオ・カメラを含むことを特徴とする上記（１）記載の記録装置。

（５）上記記録手段は上記受信手段の受信した信号によって制御される照準及びズームの設定を有する補助カメラを更に有することを特徴とする上記（４）記載の記録装置。

（６）上記記録手段は照準および強度が上記受信手段の受信した信号によって制御される良好な平行度を有するビームを放射するレーザを更に有し、上記レーザは記録した証拠に効果を生じることを特徴とする上記（４）または（５）記載の記録装置。

（７）上記記録手段は、上記受信手段の受信した信号によって制御されるプロンプト発生器と、上記プロンプト発生器によって制御され、協力者に動作を促すためのプロンプトを上記協力者に出す手段と、を更に有することを特徴とする上記（４）記載の記録装置。

（８）上記プロンプトは、ビデオ・プロンプトまたは音声プロンプトであることを特徴とする上記（７）記載の記録装置。

（９）上記記録手段は、上記受信手段の受信した信号によって制御されるプロンプト発生器と、上記プロンプト発生器によって制御され、協力者による自発的な反応を生じる知覚信号を上記協力者に対して発生する手段と、を更に有することを特徴とする上記（４）記載の記録装置。

（１０）上記知覚信号は可視信号または可聴信号であることを特徴とする上記（９）記載の記録装置。

（１１）上記予測不可能な信号を周期的に送信する承認ソースを更に有することを特徴とする上記（１）記載の記録装置。

（１２）上記信号は、物理的ランダム・プロセス、疑似ランダム・プロセス、または完全には予測することのできない公に検証可能なデータから発生されることを特徴とする上記（１１）記載の記録装置。

（１３）上記第１の承認リポジトリは上記承認ソースと組み合わされることを特徴とする上記（１１）記載の記録装置。

（１４）予測不可能な信号の承認ソースと、上記信号を保存し、上記信号を受信した時を保証する第１の承認リポジトリと、上記信号に応答し、記録中の証拠に上記信号の効果を及ぼすようにディジタル記録を作成するディジタル記録装置と、上記ディジタル記録から取り出した認証情報を保存し、上記認証情報を受け取った時を保証する第２の承認リポジトリと、を有することを特徴とする認証システム。

（１５）上記ディジタル記録を受信して上記認証情報である１つ以上のダイジェストを発生するダイジェスタを更に有することを特徴とする上記（１４）記載の認証システム。

（１６）上記ディジタル記録を格納する大容量記憶装置を更に有することを特徴とする上記（１５）記載の認証システム。

（１７）上記信号の少なくとも１つを発生した時と、上記信号によって影響を受けたディジタル記録を上記第２の承認リポジトリによって受信した時との間の時間間隔は、上記効果の組立またはシミュレーションを不可能にするほど短いことを特徴とする上記（１４）記載の認証システム。

（１８）上記ディジタル記録装置はビデオ・カメラまたは音声記録器を有することを特徴とする上記（１４）記載の認証システム。

（１９）第１の承認リポジトリに格納される送信された予測不可能な信号を受信し、該信号の効果を記録中の証拠に及ぼすステップと、上記効果を含む上記証拠を記録

し、ディジタル記録を発生するステップと、上記ディジタル記録から取り出した認証情報を第２の承認リポジトリに送信して格納するステップとを含み、上記第１の承認リポジトリに上記信号を格納した時と上記認証情報を上記第２の承認リポジトリに格納した時とによって定まる期間は、リアルタイムで上記効果をシミュレーションするのを困難または不可能にするのに十分短いことを特徴とするディジタル記録方法。

（２０）上記ディジタル記録のディジタル・ダイジェストを上記認証情報として発生するステップを更に有することを特徴とする上記（１９）記載のディジタル記録方法。

（２１）承認ソースから上記信号を周期的に送信するステップと、上記信号およびその送信時刻を受信して上記第１の承認リポジトリに格納するステップと、を更に有することを特徴とする上記（１９）記載のディジタル記録方法。

【図面の簡単な説明】

【図１】図１は本発明の好適な実施例による記録装置を示すブロック図である。

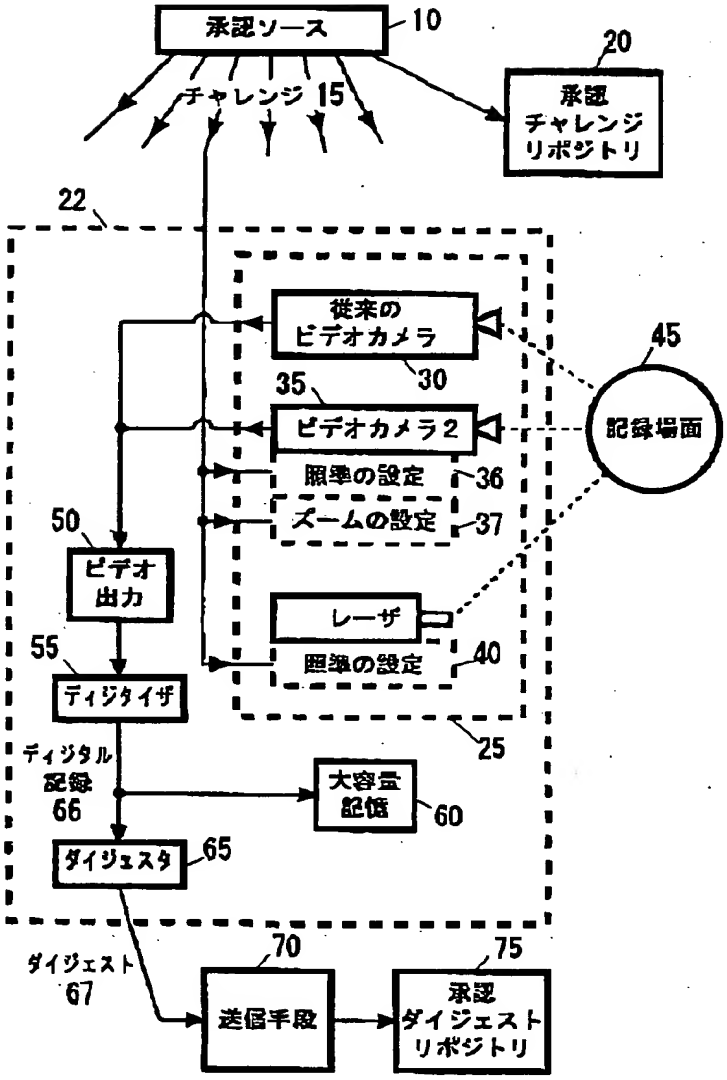
【図２】図２は、図１の装置の動作を示すフロー図である。

【図３】図３は図１の記録装置の一部の代替例を示すブロック図である。

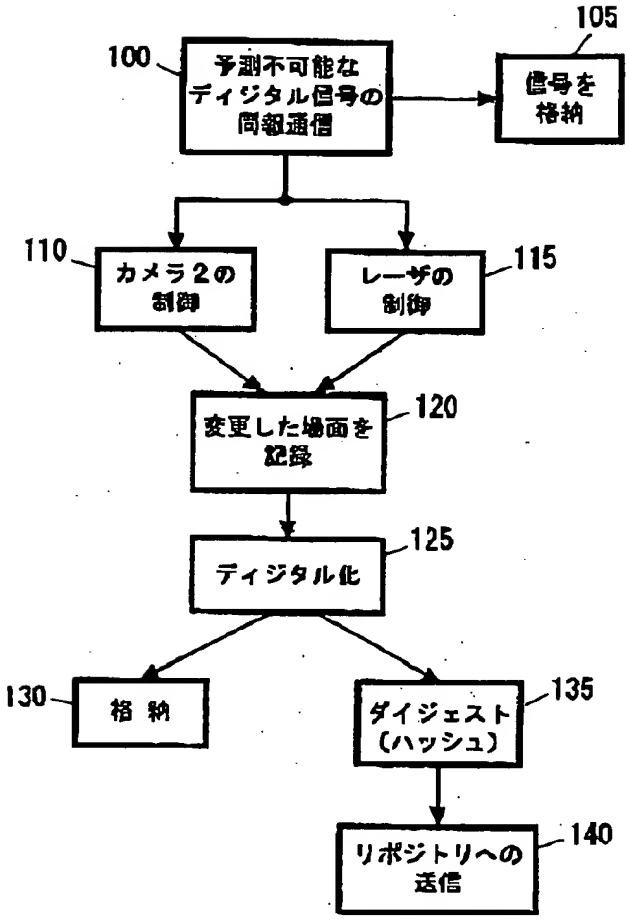
【符号の説明】

１０　承認ソース
１５　チャレンジ
２０　承認チャレンジ・リポジトリ
３０　従来のビデオカメラ
３５　従来のカメラ２
３６、４０　照準の設定
３７　ズームの設定
４５　記録場面
５０　ビデオ出力
５５　ディジタイザ
６５　ダイジェスタ
６７　ダイジェスト
７０　送信手段
７５　承認ダイジェスト・リポジトリ
３１０　モニタ
３１１　プロンプト発生器
３２０　スピーカ
３３０　投光器
３３１　可変電源
３４０　扇風機

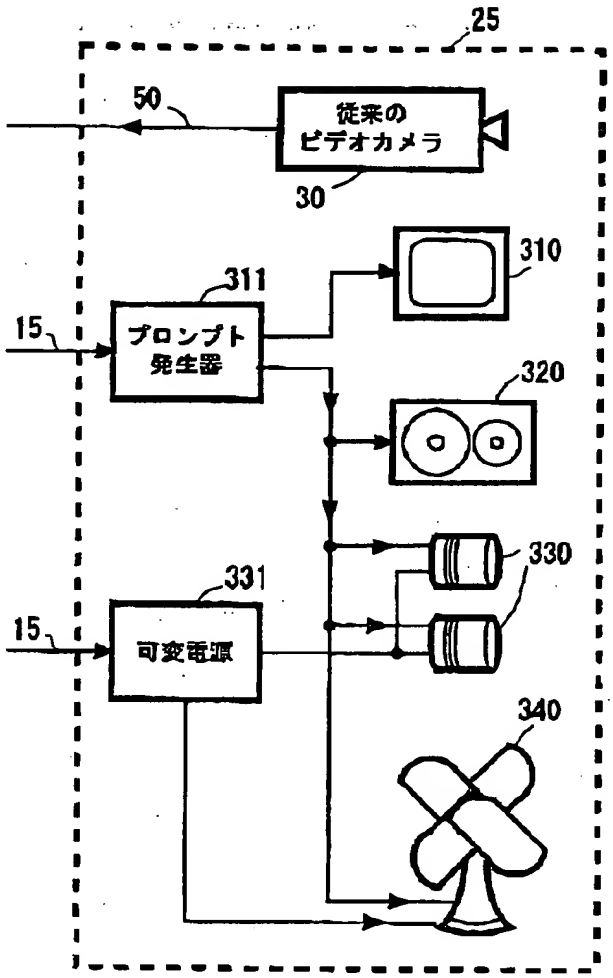
【図1】



【図2】



【図3】



フロントページの続き

(72)発明者　デヴィッド・ペーター・ディヴィンセンツォ
アメリカ合衆国10514、　ニューヨーク州　チャバックア　ベッドフォード　ロード　150　エヌ　アパートメント　ディー4

(72)発明者　ラルフ・リンスカー
アメリカ合衆国10546、　ニューヨーク州　ミルウッド　ヒドゥン　ホロウ　レーン　81